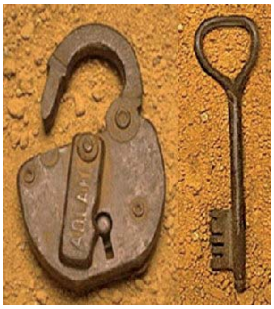


Como encriptar información en el System i

Si esta pensando en utilizar las API Cryptographic de IBM (QC3ENCDT, Qc3EncryptData) para encriptar campos de bases de datos, le interesa seguir leyendo.

Creemos que el Sistema Operativo del System i no ofrece una solución fuera de lo normal para la encriptación de campos de bases de datos, especialmente considerando los requerimientos para una administración integrada de claves, controles y pistas de auditoría. En cualquier caso, los usuarios deben decidir si deberían intentar construir su propio sistema de encriptación (Utilizando las API de IBM) o adquirir un producto especializado que encaje con sus necesidades.

Los programadores pueden pensar que construir un sistema de encriptación propio puede ser un trabajo interesante y motivador. Sin embargo, el tiempo y coste de dedicación pueden desbordar fácilmente las previsiones iniciales. Mas aun, si la solución creada no se adapta correctamente, los riesgos potenciales pueden ser extremadamente altos para una Organización. Las fugas de datos (Data breach) son una realidad que exige un alto nivel de especialización.

Se citan a continuación los puntos mas interesante a tener en cuenta cuando se esta considerando construir un sistema propio de encriptación.

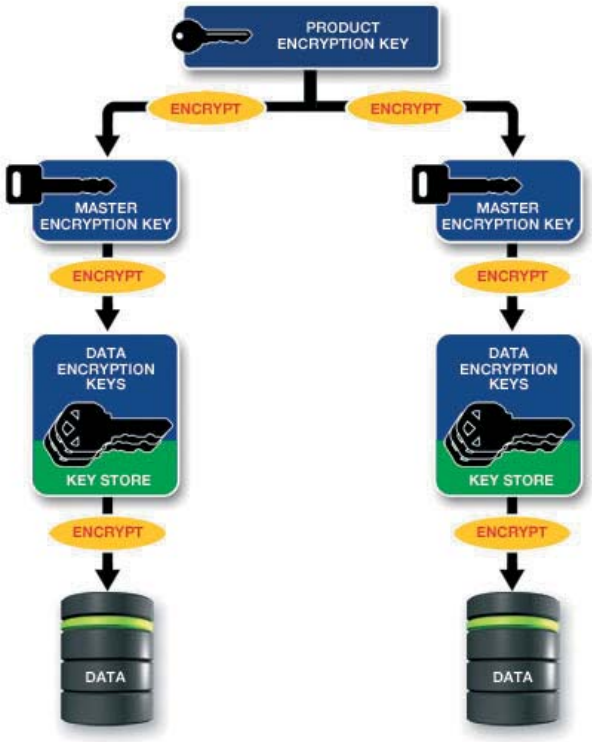
CREANDO UNA SOLUCIÓN PROPIA

Si una Organización esta considerando crear su propio sistema de encriptación, debe en primer lugar tener un buen conocimiento de todas las reglas y necesidades PCI (Payment Card Industry) y DSS (Data Security Standard) que afectan a su Organización. Su personal de desarrollo tiene que aprender como utilizar las técnicas de encriptación y desencriptación, así como convertirse en un experto en la administración de claves y en las necesidades de seguridad y auditoría.

Las Organizaciones que han tratado de crear y aplicar su propia solución han experimentado multitud de inconvenientes y deficiencias, algunos de los cuales citamos:

- Las API de encriptación de IBM tiene una pronunciada curva de aprendizaje y puede ser difícil su aplicación y también su configuración correcta.
- A menudo es necesario hacer significativos cambios en las aplicaciones para llamar las API de encriptación cuando información sensible es añadida o cambiada.
- Definiciones de campos a menudo tienen que ser cambiados para acomodar la información encriptada resultante, por ejemplo, cambiando el tipo de campo de Numérico a Alfanumérico y/o cambiando el tamaño del mismo.
- Información sensible no se encripta cuando se entra o cambia desde fuera de las aplicaciones, por ejemplo, utilizando herramientas tipo DBU o DFU.
- La administración de claves a menudo no coincide con las exigentes especificaciones PCI (Payment Card Industry) y DSS (Data Security Standard).
- Hay una falta de controles en quién crea y administra las claves.
- Las claves no están adecuadamente protegidas de usos no autorizados.
- Es difícil la rotación de claves sin reencriptar toda la información existente.
- No existen pistas de audiroría o están limitadas.
- Los propios programadores conocen demasiado del sistema adoptado incrementando el riesgo de la Organización en el caso de abandonarla.
- Una solución propia normalmente no consigue cubrir las necesidades de la Organización.

La cantidad de tiempo y dinero que serían necesarios para el desarrollo, pruebas y documentación de la solución propia de encriptación no es eficiente ni práctica en la mayor parte de los casos. Una solución propia puede también ocasionar riesgos si no se incorpora adecuada-



mente y no cumple las reglas de seguridad PCI (Payment Card Industry) y DSS (Data Security Standard).

TEMAS A CONSIDERAR AL CREAR UNA SOLUCIÓN A MEDIDA

A continuación aparecen las preguntas que una Organización debe hacerse cuando esta considerando crear su propia aplicación de encriptado en el System i. Cada pregunta viene seguida de la respuesta proporcionada utilizando una conocida aplicación externa como el Crypto Complete.

GESTIÓN CLAVES ENCRIPTACIÓN

PREGUNTA USUARIO: *¿Cómo serán creadas la Data Encryption Keys?*

RESPUESTA ATT: Crypto Complete permite que una Organización especifique si las claves pueden ser generadas aleatoriamente, generadas con passphrase (Cadena de palabras y caracteres que usted introduce para autentificarse) o entradas manualmente.

PREGUNTA USUARIO: *¿Cómo controlará que usuarios pueden crear, cambiar y borrar Data Encryption Keys?*

RESPUESTA ATT: Crypto Complete permite que una Organización especifique que usuarios (Key Officers) pueden crear, cambiar y borrar Data Encryption Keys. Incluso usuarios con autorización para *ALLOBJ o *SECADM pueden no estar autorizados a manejar Data Encryption Keys.

PREGUNTA USUARIO: *¿Cómo creará un doble control que obligue a que dos o tres personas, conociendo solo su parte de la clave, manejen conjuntamente la clave completa?*

RESPUESTA ATT: Crypto Complete permite que una Organización especifique la partes de contraseña que deben ser entradas para generar una clave Master. Cada parte de contraseña puede ser requerida para ser entrada por un único usuario. Este dispositivo de doble control de seguridad impide que un solo usuario sea capaz de reconstruir una clave por si solo.

Guardar el valor de la clave en el programa fuente o en un área de datos no cumple con los estándares PCI.

PREGUNTA USUARIO: *¿Dónde se guardarán las Data Encryption Keys en el System i?*

RESPUESTA ATT: Crypto Complete las Data Encryption Keys (DEK) en el almacén Key Stores en el que son creadas como objetos *VLDL (Validation List) en el System i. Las claves almacenadas en Key Stores son encriptadas con un Master Encryption Key y no pueden ser utilizadas sin la adecuada autoridad.

PREGUNTA USUARIO: *¿Cómo se protegerán las Data Encryption Keys de un uso no autorizado?*

RESPUESTA ATT: Crypto Complete permite que una Organización asegure el acceso al Key Stores, en donde se guardan las Data Encryption Keys, utilizando la seguridad sobre objetos del System i. Si un usuario intenta utilizar una clave de un Key Store, será debidamente registrado por el Audit. Journal del Crypto Complete.

PREGUNTA USUARIO: *¿Pueden ser vistos por programadores u otros usuarios los valores de los Data Encryption Keys?*

RESPUESTA ATT: Crypto Complete permite que una Organización especifique si los valores de las Data Encryption Keys pueden ser vistos o exportados. Por defecto, los valores de estas claves (DEK) no pueden ser vistos ni exportados y permanecen encriptados dentro del Key Stores.

PREGUNTA USUARIO: *¿Estarán las Data Encryption Keys protegidas (Encriptadas) con Master Keys? ¿Cómo se controla quién crea y administra los Master Keys?*

RESPUESTA ATT: Crypto Complete encripta las

Data Encryption Keys utilizando Master Keys. Para cada entorno pueden crearse hasta 8 Master Keys. La Organización puede indicar que usuarios (Key Officers) están autorizados para crear y manejar Master Keys.

PREGUNTA USUARIO: *¿Qué pistas de seguridad se generarán cuando las claves sean creadas, cambiadas o borradas?*

RESPUESTA ATT: Crypto Complete crea automáticamente apuntes en el log de auditoría cuando las claves son creadas, cambiadas o borradas. Estos apuntes son almacenados en fichero journal de IBM y no pueden ser modificados. Los informes de auditoría pueden ser generados por usuario, períodos de tiempo con fecha y hora y tipo de auditoría.

PREGUNTA USUARIO: *¿Cómo se hace la rotación de Data Encryption Keys? ¿Hay que reencriptar la información ya encriptada?*

RESPUESTA ATT: Crypto Complete permite que una Organización organice la rotación de Data Encryption Keys en cualquier momento sin tener que modifucar los programas fuente de las aplicaciones y sin tener que reencriptar la información encriptada existente.

PREGUNTA USUARIO: *¿Cómo se recuperarán las Data Encryption Keys en una situación de desastre o emergencia?*

RESPUESTA ATT: Crypto Complete almacena las Data Encryption Keys en los Key Stores, que son objetos con listas de validación en el sistema. La Organización deberá salvar estos objetos como parte de sus Backup normales y restaurarlos en caso de emergencia.

ENCRIPTACIÓN DE LA INFORMACIÓN E INTEGRIDAD

PREGUNTA USUARIO: *¿Qué campos deberán cambiar el tamaño para ontener los valores encriptados?*

RESPUESTA ATT: Con Crypto Complete, en la mayor parte de los casos no tendrá que aumentar el tamaño de los campos para contener valores encriptados. Si el campo a encriptar es alfanumérico y es divisible por 16 o por 24, entonces el Crypto Complete permitirá almacenar los campos encriptados en el campo existente. En otro caso, el Crypto puede almacener esos valores encriptados en un fichero externo separado, que será creado y manejado automáticamente.

PREGUNTA USUARIO: *¿Tiene que cambiarse los campos de tipo numérico a tipo alfa para almacenar los valores encriptados?*

RESPUESTA ATT: El Crypto Complete puede encriptar campos numéricos y almacenar los valores encriptados en un fichero externo separado, que será creado y manejado automáticamente. Esto evita tener que cambiar los campos numéricos en campos tipo alfa.

PREGUNTA USUARIO: *¿Qué programas tendrán que ser modificados para encriptar los valores de los campos?*

RESPUESTA ATT: El Crypto Complete puede automáticamente encriptar valores de campos cuando son añadidos o cambiados en el fichero, sin que ello requiera modificación de los programas existentes. Ello se consigue a través del uso de eficientes SQL triggers de la base de datos que capturan cualquier inserción o modificación de un campo.

PREGUNTA USUARIO: *¿Cómo se controlará que usuarios pueden encriptar o desencriptar información?*

RESPUESTA ATT: Con Crypto Complete los usuarios pueden pueden encriptar o desencriptar información si están autorizados a los objetos del Key Stores donde se contiene los Data Encryption Keys. Los Key Stores pueden ser autorizados a nivel individual, perfiles de grupo y listas de autorización.

PREGUNTA USUARIO: *¿Cómo puede encriptar información entrada a través de utilidades de bases de datos como DBU, DFU, Surveyor, etc.?*

RESPUESTA ATT: El sistema de trigger SQL utilizado por el Crypto Complete encriptará automáticamente los valores de los campos que se añadan o modifiquen en el fichero. Los triggers capturarán y encriptarán la información introducida con cualquier aplicación. utilidades de base de datos o fuentes externas, como JDBC y ODBC.

PREGUNTA USUARIO: *¿Cómo puedo estar seguro de que la información ha sido encriptada correctamente y puede ser desencriptada por usuarios autorizados?*

RESPUESTA ATT: Crypto Complete es una solución aplicada desde hace años en numerosas Empresas y entornos. Si la documentación es seguida con precisión por cualquier Organización, la información será desencriptada por los usuarios autorizados.

PREGUNTA USUARIO: *¿Cómo serán generadas las pistas de auditoría cuando información sensible es desencriptada?*

RESPUESTA ATT: Crypto Complete incluye múltiples pistas de auditoría para cumplir con los más estrictos requerimientos de seguridad. Las entradas del log de auditoría son generadas por los siguientes eventos:

- Cuando se cambia cualquier clausula de la política

de claves (Key Policy).

- Cuando usuarios autorizados (Key Officers) son añadidos, cambiados o quitados.
- Cuando se crean Master Encryption Keys (MEK).
- Cuando Key Stores son creados o modificados.
- Cuando Data Encryption Keys (DEK) son creadas, exportadas, cambiadas o borradas.
- Cuando entradas en el Field Encryption Registry son añadidas, cambiadas, quitadas, activadas o desactivadas.
- Cuando cualquier función es denegada por autoridad insuficiente.
- Cuando la información es encriptada o desencriptada con una Key que requiere log de esos eventos.

Estos apuntes son almacenados en un fichero journal de IBM y no pueden ser modificados. Los informes de auditoría pueden ser generados por usuario, períodos de tiempo con fecha y hora y tipo de auditoría.

PREGUNTA USUARIO: *¿Cómo podría su Organización recuperar las claves en un caso de emergencia?*

RESPUESTA ATT: Crypto Complete incluye una fácil y detallada documentación con los protocolos a seguir para ejecutar los Backup y Restauración de las claves en caso de emergencia. También se contempla la replicación de claves para sistemas de Alta Diponibilidad (HA).

FLEXIBILIDAD

PREGUNTA USUARIO: *Si necesita encriptar algún otro campo en el futuro ¿Se puede hacer fácilmente?*

RESPUESTA ATT: Crypto Complete, por medio del Field Encryption Registry, permite a los usuarios autorizados especificar rápidamente los campos a encriptar en sus bases de datos. Para cada campo entrado en el Registro, el usuario puede especificar el nombre de campo, el nombre del fichero, clave de encriptación y algoritmo, y si algún trigger SQL debe ser usado automáticamente para encriptar los valores del campo. Campos adicionales pueden añadirse en el Registro en cualquier momento en el futuro.

PREGUNTA USUARIO: *¿Se pueden crear claves adicionales o cambiarlas en el futuro?*

RESPUESTA ATT: Crypto Complete, por medio del Key Management, permite a los usuarios autorizados crear claves adicionales y cambiar los atributos de las existentes cuanto sea necesario. Las nuevas claves pueden ser especificadas para encriptar nuevos campos y las claves pueden ser rotadas en los campos existentes en cualquier momento.

DOCUMENTACIÓN

PREGUNTA USUARIO: *¿Existirá documentación sobre como se ha montado la solución de encriptación para que otros programadosres puedan mantenerla?*

RESPUESTA ATT: Crypto Complete incluye una amplia Guía del Usuario y también una Guía del Programador. La Guía del Usuario proporciona instrucciones detalladas de cómo utilizar la Administración de Claves y el Registro de Campos a través de Menús y Mandatos. Esta Guía incluye una sección para Iniciar el Manejo y también diagramas de ayuda, así como un apartado de Preguntas y Respuestas.

La Guía del Programador proporciona documentación de cómo manejar las API del Crypto Complete con ejemplos de programas. Ejemplos en código fuente se incluyen para facilitar la comprensión.

El personal de soporte de Linoma Software y de American Top Tools puede ser contactado para cualquier pregunta, duda o problema que se plantee.

Si otro campo necesita ser encriptado en el futuro, ¿Existe documentación de cómo un programador puede efectuar la encriptación y desencriptación correcta de ese campo?

La Guía de Usuarios indica detalladamente como configurar los campos en el Field Encryption Registry. La Guía del Programador incluye instrucciones y ejemplos de cómo desencriptar los campos en las aplicaciones.

PREGUNTA USUARIO: *¿Puede el cliente confiar en que la solución de Crypto cumple con las regulaciones Standard para la Industria para la Administración de las Claves y la protección de la Información Sensible?*

RESPUESTA ATT: Crypto Complete ha sido diseñado la mejor técnica de administración de claves y protección de datos posibles para el System i.

El sistema ha sido revisado por expertos en la materia y ha pasado todas las auditorías de seguridad de la información necesarias.

PCI STANDARDS

PREGUNTA USUARIO: *¿Cumple Crypto Complete las regulaciones citadas en las secciones 3.4, 3.5 y 3.6 del PCI Data Security Standard 1.1?*

RESPUESTA ATT: Las secciones 3.4, 3.5 y 3.6 del PCI Data Security Standard contienen requisitos para protección de información de tarjetas de crédito y para una efectiva administración de claves. Se proporciona información de cómo el fabricante atiende a esos requerimientos y cual es su objetivo.

PREGUNTA USUARIO: *¿Ha pasado la solución técnica de encriptación de Crypto la auditoría PCI?*

RESPUESTA ATT: El Crypto Complete ha sido instalado en cientos de Organizaciones y Empresas en donde ha sido sometido con éxito a auditorías PCI.

ACTUALIZACIONES SISTEMA OPERATIVO

PREGUNTA USUARIO: *¿Será compatible la aplicación Crypto Complete con con futuros releases del Sistema Operativo del System i?*

RESPUESTA ATT: El fabricante, Linoma Software, Desarrollador de Programas reconocido por IBM, lo cual le permite recibir prereleases del Sistema Operativo antes de su anuncio público. Ello permite probar el funcionamiento y acomodación de la aplicación a las novedades y modificaciones del nuevo release.

Si son necesarias algunas modificaciones del Software de Crypto para hacerlo compatible con el nuevo Sistema Operativo, se creara una nueva versión que se distribuirá entre los clientes para su incorporación cuando lo crean necesario.

INVERSIÓN / COSTES

¿Cuántas horas son requeridas por sus programadores para adquirir los conocimientos necesarios acerca de las técnicas de encriptación, administración de claves, API de IBM, etc?

¿Cuántas horas serían necesarias para cambiar todas las aplicaciones donde se necesita la encriptación de algún campo?

¿Cuántas horas serían necesarias para probar y documentar todos los cambios en las aplicaciones?

Considerando las horas necesarias a invertir, ¿Cuanto le costaría al cliente la solución de encriptar algunos campos?

Si la solución no es aplicada correctamente, ¿cuales serían los riesgos y potenciales perjuicios para la Organización?

CONCLUSIÓN

Teniendo en cuenta la cantidad de tiempo y costes de crear una solución para la encriptación de la información sensible, así como el alto riesgo y perjuicios derivados de un diseño incorrecto o incompleto, muchas Organizaciones escogen normalmente la incorporación de soluciones probadas realizadas por especialistas en la materia, comoes el caso de la solución Crypto Complete.

Sistema Integrado de Encriptación

Crypto Complete es una completa aplicación que protege la información altamente sensible alojada en su iSeries mediante la encriptación, la gestión integrada de las claves y una eficaz auditoría. Todo ello realizado a través de sus pantallas intuitivas y su tecnología probada. La encriptación se realiza a nivel de campos e incluso de backup (Librerías, objetos, ficheros, savf...).

Crypto Complete le ayudará a implementar la encriptación en su organización sin necesidad de costosos y laboriosos cambios en sus aplicaciones.

American Top Tools Tel. 93 3191612 Fax 93 3191755 att@att.es